Analyzing Extended Secret Sharing Schemes based on Share Size

Suvarna S. Thube
ME Computer
Pimpri Chinchwad College of Engineering,
Akurdi, Pune, India.

Sonali Patil
Assistant Professor
Pimpri Chinchwad College of Engineering,
Akurdi, Pune, India.

ABSTRACT
Secret sharing is the technique in which secret is distributed among *n* participants. Each participant has unique secret share. Secret can be recovered only after sufficient number of shares (*k* out of *n*) combined together. In many circumstances secret sharing has to provide additional capabilities to satisfy certain requirements. Such capabilities include proactive redistribution of shares, verifiability of the shares, robustness against cheating shareholders and general access structure.

In this paper various secret sharing schemes are discussed and critically analysed with the strengths and weaknesses introduced into these schemes on the basis of additional features, storage space, share size.

Keywords
General access structure, Secret Sharing, Proactive redistribution, Verifiability.

1. INTRODUCTION
Nowadays, use of internet is rapidly increasing. Many people prefer internet to transfer information. Sometimes sensitive data such as passwords, trade secrets, Government reports, research data, bank account details, etc. also sent through internet only. Such sensitive data needs to be protected from unauthorized access. Only recipient can get access to that data. Securing information over the internet is a recent hot issue. Hence it is necessary to protect such data from others. Cryptography, data hiding, secret sharing are the various ways to protect this information over insecure communication channel.

A secret sharing scheme is a method in which a secret, commonly a cryptography key, is divided into multiple parts called secret shares and distributed to a collection of individuals or players. The agency responsible for performing the division is often called the dealer, and in many sharing schemes it is assumed that the dealer is perfectly honest.

The following figure (1) clears idea about secret sharing. During share construction, dealer divides secret image into *n* shares also called as shadow images. Then secret image is destroyed and shares are distributed to *n* participants. To reconstruct the secret any *k* or more than those shares are combined together. Less than *k* shares cannot reconstruct the secret.

In this paper various secret sharing schemes (SSS) are studied. In some applications there is need to provide extensive features [18] to these secret sharing schemes. Few extended capabilities are also discussed in this paper. In this work, secret image sharing schemes are compared on the basis of additional capabilities, storage space and share size.

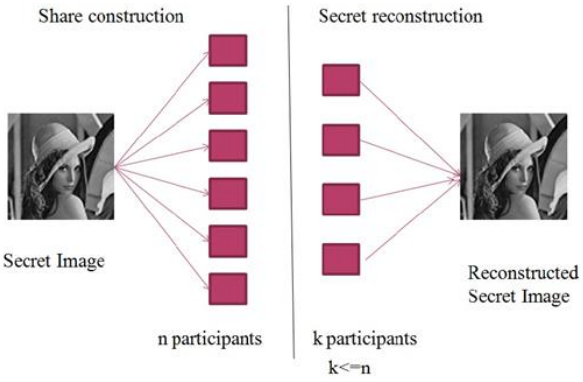

Fig 1: Concept of Secret Sharing

The remaining part of the paper is organized in different sections as follows. The literature survey is given in Section II. In Section III the description of the additional capabilities is given. Section IV discusses comparison of secret sharing schemes on various parameters. Conclusion is given in Section V.

2. LITERATURE SURVEY
In this section various secret sharing schemes discussed. It includes Shamir's secret sharing scheme, Thien and Lin's image secret sharing scheme; Li Bai's matrix projection based secret sharing schemes.

2.1 Shamir's Secret Sharing Scheme
Concept of secret sharing firstly invented by Adi Shamir [1] and George Blakley [2] in 1979 independently. Scheme proposed by both is based on different concepts. Shamir's scheme is based on polynomial technique while Blakley's scheme based on hyper plane concept. Secret sharing includes two main phases namely share construction and secret reconstruction phase. Shamir's scheme works as follows.

Share Construction:

For share construction, threshold (*k*, *n*) and secret value S is required. Then polynomial function of an order (*k*-1) is constructed as shown in equation (1).

$$f(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_{k-1} x^{k-1} (mod\ p) \quad \ldots(1)$$

In above equation, constant term d_0 is replaced with secret value S. The other coefficients such as, d_1, d_2, …, d_{k-1} are any random values.

Secret shares are the pairs of values (x_i, y_i), where $y_i = f(x_i)$ for $1 \leq i \leq n$ and $0 < x_1 < x_2 \ldots < x_n < n$ -1.

After share construction polynomial function f(x) is destroyed and shares are distributed among *n* number of participants.

Secret Reconstruction:

During secret reconstruction any *k* shares are collected. Then, secret value is computed using Lagrange's interpolation formula. Equation (2) shows the Lagrange's interpolation formula which gives polynomial function f(x).

$$f(x) = \sum_{j=1}^{k} \left(y_{i_j} \prod_{1<-t<-k, t\neq j} \frac{x - x_{i_t}}{x_{i_j} - x_{i_t}} \right) mod\ p \ldots (2)$$

The constant term in equation f(x) is our original secret value. Equation (2) can be further simplified as whole equation is not needed. Simplified equation is shown in equation (3) which directly gives constant term i.e. secret value S.

$$d_0 = \sum_{j=1}^{k} \left(y_{i_j} \prod_{1<-t<-k, t\neq j} \frac{x_{i_t}}{x_{i_t} - x_{i_j}} \right) mod\ p \quad \ldots (3)$$

2.2 Thien and Lin's Secret Sharing Scheme

Thien and Lin proposed image secret sharing scheme. It is mainly based on concept of Shamir's secret sharing scheme. In Shamir's scheme, (*k*-1) random numbers and the secret value together form the polynomial equation f(x). Thien and Lin suggested that instead of taking (*k*-1) random numbers pick *k* image pixels. It works as follows.

Share Construction:

i. Read secret image S.
ii. Supress all pixels values to 250, which are greater than 250.
iii. Permute the secret image S.
iv. Sequentially take distinct *k* pixels of image S which are not already taken and form polynomial equation of order (*k*-1).
v. Then generate *n* pixels for *n* shadow images.
vi. Repeat steps (iv) and (v) until all pixels of image not get covered.
vii. Distribute *n* shadows among participants.

Secret Reconstruction:

i. Collect any distinct *k* shadow images.
ii. Pick first but not yet used pixel from each shadow image.
iii. Using Lagrange's interpolation formula as shown in equation (2) get the coefficients of polynomial function f(x).
iv. Place these coefficients sequentially to form permuted image.
v. Pixels of permuted image inversely permuted to get the original one.

This scheme may give some distorted secret because of pixel suppression. Thien and Lin also proposed lossless image secret sharing scheme. In lossless scheme we have to keep track of pixels whose values are greater than 250.

2.3 Li Bai's Strong Ramp Secret Sharing Scheme

Li Bai proposed a strong (*k*, *n*) threshold based ramp secret sharing scheme in 2006. It is based on matrix projection technique. For square image of size m × m, this scheme reduces share size to m × 1. It works as follows for secret image of size m × m. Image must be square image.

Share Construction:

i. For m × m image size take random matrix A of size m × *k* having rank *k*.
ii. Choose *n* random vectors of size *k* × 1 out of which any *k* vector must be independent.
iii. Shares calculated as,
$$v_i = (A \times x_i)\ mod\ p\ ,\ 1 \le i \le n\ .$$
iv. Compute projection matrix $.
$$\$ = A \times (A' \times A)^{-1} \times A'$$
v. Compute remainder (public) matrix.
$$R = (S - \$) mod\ p$$
vi. Destroy matrix A, vectors x_i, projection matrix $ and secret S.
vii. Distribute *n* shares v_i among shareholders. Make remainder matrix R public.

Secret Reconstruction:

i. Select any distinct *k* shares and combine them to form matrix B.
$$B = [v_1\ v_2\ \ldots\ v_k]$$
ii. Compute projection matrix $.
$$\$ = B \times (B' \times B)^{-1} \times B'$$
iii. Compute secret image S.
$$S = (R + \$) mod\ p$$

2.4 Li Bai's Reliable Secret Sharing Scheme

In previous Strong Ramp method there is one public matrix with same size as secret image. But it may lead to single point failure. If we lost public matrix or if it get corrupted, we cannot reconstruct the secret image. To overcome this problem, Li Bai suggested a reliable scheme incorporating with it Thien and Lin's [3] image SSS. It increases share size but still it is less than original. It works as follows.

Share Construction:

First five steps are same as previous strong ramp scheme.

i. For m × m image size take random matrix A of size m × *k* having rank *k*.
ii. Choose *n* random vectors of size *k* × 1 out of which any *k* vector must be independent.
iii. Shares calculated as,
$$v_i = (A \times x_i)\ mod\ p\ ,\ 1 \le i \le n\ .$$
iv. Compute projection matrix $.
$$\$ = A \times (A' \times A)^{-1} \times A'$$
v. Compute remainder (public) matrix.
$$R = (S - \$) mod\ p$$
vi. Now, instead of making R matrix public secretly share it using Thien and Lin's image SSS.
It will give *n* shadow images of R of size m × (m/*k*).
$G_1, G_2, \ldots, G_n$ are shadow images of R image.
vii. To get image share, combine shares v and shadow image G such as ,
$Sh_i = [v_i\ G_i]$
viii. Destroy matrix A, vectors x_i, v_i, projection matrix $, remainder matrix R ,$G_i$ and secret S.
ix. Distribute *n* shares Sh among shareholders.

Secret Reconstruction:

i. Select any *k* distinct shares and take first column of each share to form matrix B.

$$B = [v_1\ v_2\ \dots\ v_k]$$

ii. Compute projection matrix $.

$$\$ = B \times (B \times B)^{-1} \times B'$$

iii. Using Thien and Lin's image SSS reconstruct R matrix.

iv. Compute secret image S.

$$S = (R + \$) mod\ p$$

3. EXTENDED CAPABILITIES

In many circumstances, secret sharing has to provide more flexibility and functionality. The requirements for different extra functionalities of SSS are often contradictory to each other which make construction of a SSS with several additional features a challenge. In many circumstances secret sharing has to provide additional capabilities to satisfy certain requirements. Such capabilities include proactive redistribution of shares, verifiability of the shares, robustness against cheating shareholders and general access structure.

Various extended capabilities are explained in this section.

3.1 Threshold Secret Sharing

Under this scheme, the message M is divided into *n* pieces M_1, M_2, M_3,…, M_n, with or without transformation of the message, in such a way that, for a specified *k*, ($2 \leq k \leq n$),

1. Knowledge of any *k* or more pieces M_i makes M computable.
2. Knowledge of any *k*-1 or fewer M_i pieces leaves M completely undetermined (in the sense that all its possible values are equally likely).

Such a scheme is called a (*k*, *n*)-threshold scheme. The parameter *k*-*n* is called the threshold value

There may be some situations where all participants can not present at a same time, in such circumstances it is required that specified number of participants must come together to reveal secret.

3.2 Proactive Secret Sharing

Proactive Secret Sharing (PSS) is a scheme that allows generating new set of shares for the same secret from the old shares without reconstructing the secret. Using PSS, all the shares are refreshed so that old shares become useless. Concept of PSS is proposed by Herzberg et.al. in [6]. In this paper they give general idea of proactive secret sharing and how to manage information leakage. Saria Islam et.al. [7] introduced a new scheme for extending the Shamir's scheme on proactive network. Li Bai [8] proposed a proactive scheme in matrix projection secret sharing scheme.

3.3 Verifiable Secret Sharing

Verifiable schemes seek to prevent individuals from lying about their share in order to obtain information about the other shares. According to the Wikipedia entry, verifiable schemes allow the participants to be certain that no other participant is lying about the contents of their share, up to a reasonable probability of error. Benaloh [9] introduced verifiable secret sharing in 1986. Verifiability is provided to Shamir's Secret Sharing scheme. For verification purpose he had used homomorphism property. Feldman [10] has proposed a non-interactive scheme for achieving verifiability in Shamir's threshold secret sharing scheme. Z. Wang et al. [11] proposed a verifiable secret sharing scheme for binary images using watermarking. S. Patil, P. Deshmukh [12] proposed a scheme to verify reconstructed secret. This scheme is based on Li Bai's reliable image secret sharing scheme.

3.4 General Access Structure

In practice, it is often needed that only certain specified subsets of the participants should be able to recover the secret. The Access structure describes all the authorized subsets to design the access structure with required capabilities. The goal of the general access structure secret sharing scheme is to provide the flexibility to decide which specified subsets of participants will able to reconstruct the original secret and which subsets cannot. Benaloh and Leichter [13] proposed generalized secret sharing. S.Patil and P. Deshmukh [14] proposed general access structure for matrix projection based secret sharing.

3.5 Cheater Identification

Cheater identification scheme is used to identify the cheater among several participants. There may be possibility that shares will get changed during transmission or get changed by someone purposely. So, we need to identify who is cheater? There are some schemes which support this feature. Harn and Lin [15] proposed cheater identification method for Shamir's scheme. Zhao et al. [16] proposed new lossless secret sharing scheme to identify cheaters in image secret sharing. S. Patil and P. Deshmukh [17] proposed new approach to identify cheaters in matrix projection based secret sharing.

4. COMPARATIVE STUDY

4.1 Storage Space V/s Image size

From below graph shown in figure (2), we can see that as image size and threshold increases total storage space for shares is also increases. For Shamir's scheme, storage space is more, while Thien and Lin's scheme is better than Shamir's scheme. Li Bai's matrix projection based reliable scheme requires storage space equivalent to that of Thien and Lin's scheme. Li Bai's strong ramp scheme is much better than other methods. In case of Thien and Lin's scheme and Li Bai's reliable scheme storage space reduces as threshold gets increased. For varying threshold value storage space is consistent for other methods but for varying image size it differs. Graph clearly shows that Li Bai's strong ramp scheme takes less storage space.

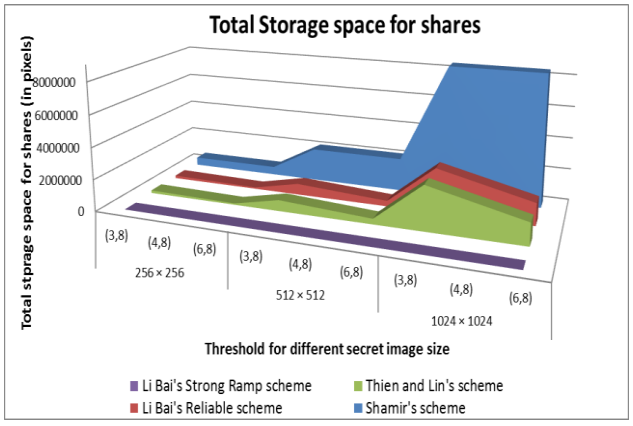

Fig 2: Comparison of schemes based on total storage space for shares

4.2 Share size V/s Threshold

From the graph shown in Figure (3), we can see that for varying threshold value size of shares is constant in Shamir's scheme and Li Bai's strong ramp scheme. For Thien and Lin's scheme and Li Bai's reliable scheme share size decreases as threshold get increased. This is the advantage of Thien and Lin's scheme and Li Bai's reliable scheme over Shamir's scheme. For Shamir's scheme, share size is same as secret image size but Li Bai's strong ramp scheme has very small share size.

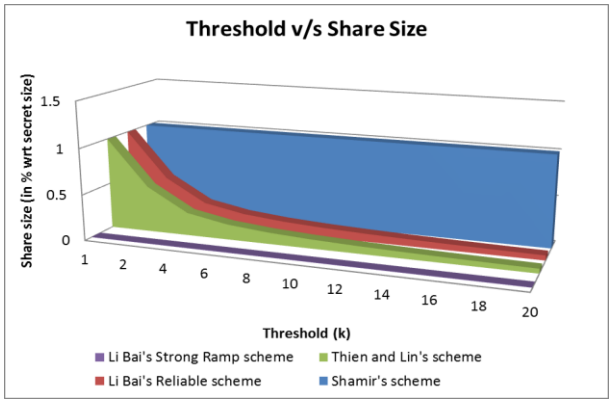

Fig 3: Comparison of schemes based on share size

4.3 Comparison based on different features

Table (1) shows the comparative study of different schemes based on different parameters. From Table (1), we can see that, the schemes which are based on matrix projection are better than any other schemes. They also support extended capabilities. Secret sharing parameter shows whether secret sharing is supported for single secret or multiple secret. Li Bai's matrix projection based scheme is supported for multiple secrets. A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S whatsoever, in the information theoretic sense. Shamir's scheme is regarded as a perfect secret sharing scheme. Li Bai's scheme is also ramp scheme but not perfect, but Thien and Lin's scheme is not perfect. Underlying technique is the method, the scheme uses to generate shares and reconstruct secret from shares. Other parameters are the additional capabilities supported by schemes.

5. CONCLUSION

In upcoming years, the secret sharing schemes will become the most promising solution in information security domain. The purpose of this study is to focus on storage requirement for different schemes and the additional features supported by them. This study shows that, Li Bai's scheme supports most of the features also storage requirement is less for the same.

Table 1: Comparison of secret sharing schemes based on different parameters

Scheme / Parameter	Shamir's SSS	Thien and Lin's SSS	Li Bai's Strong Ramp scheme	Li Bai's Reliable scheme
Secret Sharing	Single	Single	Multiple	Multiple
Perfect	Yes	No	No	Yes
Computational Complexity	More	More	Less	More
Underlying Technique	Polynomial	Polynomial	Matrix Projection	Matrix Projection and Polynomial
Renewal of Shares	No	No	Yes	Yes
Verifiability	No	No	Yes	Yes
Cheater Identification	Yes	Yes	No	Yes
General Access Structure	No	No	Yes	No

6. REFERENCES

[1] Adi Shamir, "How to share a secret", Communication of the ACM, Volume 22, No. 11, PP. 612- 613, Nov 1979.

[2] G. R. Blakey, "Safeguarding Cryptographic Keys", Proceedings of National Computer Conference, American Federation of Information, 1979.

[3] Thien and Lin, "Secret image sharing", Computers and Graphics, Volume. 26, No.5, PP. 765-770, 2002.

[4] Li Bai, "A Strong Ramp Secret Sharing Scheme Using Matrix Projection", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006.

[5] Li Bai ,"A Reliable (*k*, *n*) Image Secret Sharing Scheme", IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006.

[6] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Secret Sharing Or: How to Cope with Perceptual Leakage", Springer- Verlag, 1998.

[7] Saria Islam, A. S. M. Mahmudul Hasan, "Implementation of Shamir's Secret Sharing on Proactive Network", International Journal of Applied Information Systems, Volume 6- No. 2, Sep 2013.

[8] Li Bai, XuKai Zou, "A Proactive Secret Sharing Scheme in Matrix Projection Method", International Journal of Security and Networks, Volume. 4, No. 4, PP. 201-209, 2009.

[9] J. C. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Proceedings of CRYPTO86 Springer, Berlin, PP. 251260, 1986.

[10] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", IEEE Symposium on Foundations of Computer Science, PP. 427437, 1987.

[11] Z. Wang et. al., "Sharing a Secret Image in Binary Images with Verification", Journal of Information Hiding and Multimedia Signal Processing, Volume 2, No. 1, Jan 2011.

[12] Sonali Patil, P. Deshmukh, "Verifiable Image Secret Sharing in Matrix Projection Using Watermarking", International conference on Circuits, Systems, Communication and Information Technology Applications, IEEE, 2014.

[13] J. Benaloh, J. Leichter. "Generalized Secret Sahring and Monotone Functions", Springer- Verlag, 1998.

[14] Sonali Patil, Prashant Deshmukh, "General Access Structure Secret Sharing in Matrix Projection", International Journal of Computer Applications, Volume 107, No. 13, Dec 2014.

[15] L. Harn, C. Lin, "Detection and identification of cheaters in (t, *n*) secret sharing scheme", Springer Science + Business Media, Designs, Codes and Cryptography, Volume 52, PP. 15-24, 2009.

[16] Rong Zhao, Jian-jie Zhao, Fang Dai, Feng-qun Zhao, A new image secret sharing scheme to identify cheaters, Computer Standards and Interfaces 31, pp. 252257, 2007.

[17] Sonali Patil, Prashant Deshmukh, "Image Secret Sharing with Identification of Cheaters", IEEE International Conference on Advances in Engineering &Technology Research (ICAETR - 2014), Aug 2014.

[18] Sonali Patil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications, volume. 46, no. 19, pp. 6-10, 2012.